Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0321

Meerdere kwetsbaarheden verholpen in IBM AIX en IBM PowerVM VIOS

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-08-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

IBM heeft kwetsbaarheden verholpen in AIX en PowerVM VIOS. Ook heeft IBM eerdere kwetsbaarheden in, onder andere, DB2, WebSphere, Oracle producten als Java en GraalVM, PostgreSQL, OpenSSH en Perl verholpen voor de producten geproduceerd voor AIX.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service
- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (root/admin-rechten)
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens
- Manipulatie van gegevens
- Verhogen van privileges

Oplossingen

De leveranciers hebben updates uitgebracht voor PostgreSQL, IBM AIX, IBM PowerVM VIOS, Perl modules, OpenSSH, Oracle Java SE, Oracle GraalVM, OpenJDK, IBM Db2 Client en Server, en Oracle Communications Cloud Native Core Certificate Management om de beschreven kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.ibm.com/support/pages/node/7283858

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-12817	4.3 MEDIUM
CVE-2025-12818	7.5 HIGH
CVE-2025-15649	5.5 MEDIUM

CVE-2026-2003	4.3 MEDIUM
CVE-2026-2004	8.8 HIGH
CVE-2026-2005	8.8 HIGH
CVE-2026-2006	8.8 HIGH
CVE-2026-6472	5.4 MEDIUM
CVE-2026-6473	8.8 HIGH
CVE-2026-6474	4.3 MEDIUM
CVE-2026-6475	8.8 HIGH
CVE-2026-6477	8.8 HIGH
CVE-2026-6478	8.2 HIGH
CVE-2026-6637	8.8 HIGH
CVE-2026-8368	6.5 MEDIUM
CVE-2026-8400	8.1 HIGH
CVE-2026-8829	7.5 HIGH
CVE-2026-12087	9.1 CRITICAL
CVE-2026-14970	7.5 HIGH
CVE-2026-15061	8.2 HIGH
CVE-2026-15065	9.1 CRITICAL
CVE-2026-15068	9.9 CRITICAL
CVE-2026-15078	8.1 HIGH
CVE-2026-16243	5.7 MEDIUM
CVE-2026-16439	5.8 MEDIUM
CVE-2026-16441	6.9 MEDIUM

CVE-2026-16656	9.8 CRITICAL
CVE-2026-16686	8.2 HIGH
CVE-2026-16690	7.5 HIGH
CVE-2026-16703	7.8 HIGH
CVE-2026-16706	7.5 HIGH
CVE-2026-16814	8.8 HIGH
CVE-2026-16816	9.9 CRITICAL
CVE-2026-16817	7.5 HIGH
CVE-2026-16818	7.5 HIGH
CVE-2026-16819	7.7 HIGH
CVE-2026-16822	9.3 CRITICAL
CVE-2026-16824	7.5 HIGH
CVE-2026-16825	4.2 MEDIUM
CVE-2026-16827	5.9 MEDIUM
CVE-2026-16829	5.3 MEDIUM
CVE-2026-16831	7.5 HIGH
CVE-2026-16833	5.3 MEDIUM
CVE-2026-16834	9.8 CRITICAL
CVE-2026-16836	7.5 HIGH
CVE-2026-16837	7.5 HIGH
CVE-2026-16838	7.0 HIGH
CVE-2026-16839	9.4 CRITICAL
CVE-2026-16840	9.8 CRITICAL

CVE-2026-16841	8.8 HIGH
CVE-2026-16842	8.8 HIGH
CVE-2026-16844	8.8 HIGH
CVE-2026-16845	9.8 CRITICAL
CVE-2026-16846	6.5 MEDIUM
CVE-2026-16847	8.8 HIGH
CVE-2026-16848	8.8 HIGH
CVE-2026-16849	4.3 MEDIUM
CVE-2026-16850	8.8 HIGH
CVE-2026-16851	7.4 HIGH
CVE-2026-16852	7.5 HIGH
CVE-2026-16855	5.5 MEDIUM
CVE-2026-16857	8.2 HIGH
CVE-2026-16862	9.8 CRITICAL
CVE-2026-16864	9.8 CRITICAL
CVE-2026-16865	8.8 HIGH
CVE-2026-16866	4.8 MEDIUM
CVE-2026-16869	7.8 HIGH
CVE-2026-16872	9.8 CRITICAL
CVE-2026-16873	7.8 HIGH
CVE-2026-16874	7.8 HIGH
CVE-2026-16875	7.8 HIGH
CVE-2026-16877	8.8 HIGH

CVE-2026-16882	9.8 CRITICAL
CVE-2026-16883	5.5 MEDIUM
CVE-2026-16885	9.8 CRITICAL
CVE-2026-16886	4.3 MEDIUM
CVE-2026-16888	3.7 LOW
CVE-2026-16890	3.6 LOW
CVE-2026-16891	3.3 LOW
CVE-2026-16894	9.8 CRITICAL
CVE-2026-16897	4.4 MEDIUM
CVE-2026-16901	8.8 HIGH
CVE-2026-16903	9.6 CRITICAL
CVE-2026-16909	8.8 HIGH
CVE-2026-16911	8.8 HIGH
CVE-2026-16913	9.8 CRITICAL
CVE-2026-16914	6.7 MEDIUM
CVE-2026-16917	9.8 CRITICAL
CVE-2026-16919	9.8 CRITICAL
CVE-2026-16922	7.0 HIGH
CVE-2026-16923	7.0 HIGH
CVE-2026-16924	7.5 HIGH
CVE-2026-16925	7.1 HIGH
CVE-2026-16926	9.1 CRITICAL
CVE-2026-16927	7.3 HIGH

CVE-2026-16928	7.5 HIGH
CVE-2026-16932	8.8 HIGH
CVE-2026-16934	8.8 HIGH
CVE-2026-16935	7.8 HIGH
CVE-2026-16936	8.8 HIGH
CVE-2026-16937	7.8 HIGH
CVE-2026-16943	8.2 HIGH
CVE-2026-16944	6.7 MEDIUM
CVE-2026-16945	7.8 HIGH
CVE-2026-16946	7.8 HIGH
CVE-2026-16951	6.7 MEDIUM
CVE-2026-16952	5.5 MEDIUM
CVE-2026-16958	6.5 MEDIUM
CVE-2026-16964	6.5 MEDIUM
CVE-2026-16972	6.5 MEDIUM
CVE-2026-16973	5.5 MEDIUM
CVE-2026-16980	6.3 MEDIUM
CVE-2026-16989	7.1 HIGH
CVE-2026-16991	7.8 HIGH
CVE-2026-16996	8.8 HIGH
CVE-2026-16997	7.8 HIGH
CVE-2026-17000	8.1 HIGH
CVE-2026-17003	7.7 HIGH

CVE-2026-17006	8.3 HIGH
CVE-2026-17007	6.7 MEDIUM
CVE-2026-17009	4.7 MEDIUM
CVE-2026-17024	7.7 HIGH
CVE-2026-17040	9.8 CRITICAL
CVE-2026-17060	8.1 HIGH
CVE-2026-17118	9.8 CRITICAL
CVE-2026-17120	5.3 MEDIUM
CVE-2026-17121	7.5 HIGH
CVE-2026-17122	9.8 CRITICAL
CVE-2026-17124	7.8 HIGH
CVE-2026-17136	9.8 CRITICAL
CVE-2026-17138	8.1 HIGH
CVE-2026-17141	9.8 CRITICAL
CVE-2026-17142	9.8 CRITICAL
CVE-2026-17145	9.8 CRITICAL
CVE-2026-17152	9.8 CRITICAL
CVE-2026-17157	9.8 CRITICAL
CVE-2026-17159	7.5 HIGH
CVE-2026-17160	9.8 CRITICAL
CVE-2026-17163	7.5 HIGH
CVE-2026-17165	7.5 HIGH
CVE-2026-17168	8.5 HIGH

CVE-2026-17170	7.5 HIGH
CVE-2026-17171	7.8 HIGH
CVE-2026-17195	6.5 MEDIUM
CVE-2026-17422	9.3 CRITICAL
CVE-2026-17423	7.7 HIGH
CVE-2026-17424	4.8 MEDIUM
CVE-2026-17425	7.5 HIGH
CVE-2026-17436	8.8 HIGH
CVE-2026-18670	8.2 HIGH
CVE-2026-18716	7.9 HIGH
CVE-2026-18822	4.4 MEDIUM
CVE-2026-18824	8.4 HIGH
CVE-2026-18828	5.4 MEDIUM
CVE-2026-18832	8.8 HIGH
CVE-2026-18835	9.9 CRITICAL
CVE-2026-18840	8.2 HIGH
CVE-2026-18842	8.4 HIGH
CVE-2026-19437	8.1 HIGH
CVE-2026-19442	8.2 HIGH
CVE-2026-19446	7.5 HIGH
CVE-2026-19448	6.5 MEDIUM
CVE-2026-19449	8.8 HIGH
CVE-2026-19653	6.5 MEDIUM

CVE-2026-19783	6.7 MEDIUM
CVE-2026-22007	2.9 LOW
CVE-2026-22013	5.3 MEDIUM
CVE-2026-22016	7.5 HIGH
CVE-2026-22018	3.7 LOW
CVE-2026-22021	5.3 MEDIUM
CVE-2026-34268	2.9 LOW
CVE-2026-41254	7.5 HIGH
CVE-2026-46968	5.9 MEDIUM
CVE-2026-47010	3.7 LOW
CVE-2026-47021	5.3 MEDIUM
CVE-2026-47027	5.3 MEDIUM
CVE-2026-47057	7.5 HIGH
CVE-2026-47058	7.4 HIGH
CVE-2026-47059	3.7 LOW
CVE-2026-47063	7.5 HIGH
CVE-2026-48959	7.5 HIGH
CVE-2026-48962	7.8 HIGH
CVE-2026-59995	5.4 MEDIUM
CVE-2026-59996	5.4 MEDIUM
CVE-2026-59997	5.4 MEDIUM
CVE-2026-59999	7.5 HIGH
CVE-2026-60000	7.5 HIGH

CVE-2026-60001	6.5 MEDIUM
CVE-2026-60002	9.4 CRITICAL
CVE-2026-60147	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-61	UNIX Symbolic Link (Symlink) Following
CWE-73	External Control of File Name or Path
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-125	Out-of-bounds Read
CWE-128	Wrap-around Error

CWE-129	Improper Validation of Array Index
CWE-134	Use of Externally-Controlled Format String
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-242	Use of Inherently Dangerous Function
CWE-248	Uncaught Exception
CWE-269	Improper Privilege Management
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-287	Improper Authentication
CWE-295	Improper Certificate Validation
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-312	Cleartext Storage of Sensitive Information
CWE-319	Cleartext Transmission of Sensitive Information
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-347	Improper Verification of Cryptographic Signature
CWE-348	Use of Less Trusted Source
CWE-358	Improperly Implemented Security Check for Standard
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-369	Divide By Zero
CWE-385	Covert Timing Channel
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release

CWE-407	Inefficient Algorithmic Complexity
CWE-416	Use After Free
CWE-426	Untrusted Search Path
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
CWE-476	NULL Pointer Dereference
CWE-502	Deserialization of Untrusted Data
CWE-522	Insufficiently Protected Credentials
CWE-611	Improper Restriction of XML External Entity Reference
CWE-674	Uncontrolled Recursion
CWE-693	Protection Mechanism Failure
CWE-696	Incorrect Behavior Order
CWE-707	Improper Neutralization
CWE-758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-805	Buffer Access with Incorrect Length Value
CWE-822	Untrusted Pointer Dereference
CWE-825	Expired Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-908	Use of Uninitialized Resource
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input
CWE-1287	Improper Validation of Specified Type of Input
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

IBM
AIX
AIX, PowerVM VIOS

Disclaimer